rfc4422

Simple Authentication and Security Layer (SASL)

SASL est un framework fournissant des services d'authentification et de sécurité de données dans des protocoles orienté connexion utilisant des mécanismes remplaçable. SASL fournis une interface structurée entre les protocoles et les mécanismes. SASL fournis également un protocole pour sécuriser les échanges. SASL est conçu pour permettre à de nouveaux protocoles de réutiliser les mécanismes existants.

SASL fournis une couche d'abstraction entre les protocoles et les mécanismes. Pour utiliser SASL, chaque protocole fournis une méthode pour identifier le mécanisme à utiliser, une méthode pour échanger les challenges et une méthode pour la communication. Chaque mécanisme SASL définis une série de server-challenge et client-response qui fournissent les services d'authentification et de négociation de sécurisation des données.

Concept d'identité

SASL nécessite 2 identités :

1) L'identité associé avec les accréditifs (authentication identity)

2) L'identité qui agis en tant que (authorization identity)

Le client fournis ses accréditifs (qui inclus ou implique un authentication identity) et optionnellement, une chaîne de caractère représentant l'authorization identity. Quand cette chaîne est omis ou vide, le client agis comme identité associé avec les accréditifs.

Le serveur vérifie les accréditifs du clients et vérifie que l'identité qu'il associe avec les accréditifs du client (authorization idenity) a le droit d'agir comme authorization identity. Si une des vérifications échoue, l'échange SASL échoue.

Échange d'authentification

Chaque échange d'authentification consiste d'un message du client vers le serveur demandant une authentification via un mécanisme particulier, suivi par une ou plusieurs paires de challenges du serveur et de réponse du client, suivis par un message du serveur indiquant la sortie de l'échange d'authentification.

Exemple d'échange

C : Request authentication exchange

S : Initial challenge

C : Initial response

<additional challenge/response messages>

S : Outcome of authentication exchange

Certains mécanismes spécifient que le client envoie une réponse initiale dans la requête. Plusieurs variantes sont possible.

Nommage des mécanismes

les mécanismes SASL sont nommés par des chaînes de caractère, de 1 à 20 caractère de long, en ASCII noté (ABNF) :

```
sasl-mech = 1*20mech-char
mech-char = UPPER-ALPHA / DIGIT / HYPHEN / UNDERSCORE

UPPER-ALPHA = %x41-5A ; A-Z (uppercase only)
DIGIT = %x30-39 ; 0-9
HYPHEN = %x2D ; hyphen (-)
UNDERSCORE = %x5F ; underscore (_)
```

Négociation de mécanisme

La négociation des mécanismes est spécifique au protocole. Généralement, un protocole spécifie que le serveur avertis le client des mécanismes disponibles et supportés. Le client choisira le meilleur protocole de cette liste qu'il supporte.

Demande d'échange d'authentification

L'échange d'authentification est initié par le client en demandant une authentification via le mécanisme qu'il spécifie. Le client envoie une message contenant le nom du mécanisme au serveur. Les particularité du message sont spécifiques au protocole. Noter que le nom du mécanisme n'est pas protégé par le mécanisme.

Challenges and Responses

Les challenges et réponse sont imbriqués dans des messages de protocole. Le mécanisme peut être :

- Authentifier le client auprès du serveur
- authentifier le serveur auprès du client
- Transférer une chaîne authorization identity
- Négocier une couche de sécurité
- Fournir d'autres services.

La négociation de couche de sécurité implique la négociation de services de sécurité à fournir dans la couche et comment ces services sont fournis. Après avoir reçu une requête d'authentification ou une réponse d'un client, le serveur peut fournir un challenge, annuler l'échange, ou indiquer la sortie de l'échange. Après avoir reçu un challenge, un mécanisme client peut fournir une réponse ou annuler l'échange.

Chaîne d'identité d'authorisation

Cette chaîne est une séquence de caractères unicode représentant l'identité qui qui agis en tant que. Si cette chaîne est absente, le demandeur agis en tant qu'identité que le serveur associe avec les accréditifs du client. Une chaîne non vide indique que le client souhaite agir en tant qu'identité représentée par la chaîne.

Annuler l'échange

Un client ou un serveur peut annuler l'échange.

Fin de l'authentification

La conclusion de l'échange, le serveur envoie un message spécifique au protocole, au client indiquant la sortie de l'échange. La sortie est un échec si :

- L'échange d'authentification a échoué pour une quelconque raison
- Les accréditifs du client n'ont pu être vérifiés
- Le serveur ne peut associer une identité avec les accréditifs du client
- L'authorization Identity fournie est mal formaté
- L'identité associé avec les accréditifs du client n'est pas autorisé à agir en tant qu'authorization identity
- La couche sécurité demandée (ou son absence) n'est pas disponible et n'est pas utilisable par le client et/ou le serveur

Le protocole peut inclure des données additionnelles dans le message.

Couches de sécurité

Les mécanismes SASL peuvent offrir une grande variété de services dans les couches de sécurité, incluant l'intégrité des données et la confidentialité des données. Si la couche de sécurité est négociée dans l'échange, la couche n'est installée par le serveur qu'après le message de sortie d'échange.

Authentification multiple

Sans être explicitement permis dans le protocole, seul un échange d'authentification réussis peut se produire dan une sessions. Quand plusieurs authentifications sont permis, en aucun cas il ne peut y avoir plusieurs couche de sécurité simultanés. Si une couche de sécurité est effective, et qu'une seconde négociation sélectionne une autre couche de sécurité, la seconde couche remplace la première.

Protocol requirements

Pour qu'un protocole offre des services SASL, ses spécifications doivent fournir les informations suivantes :

1) un nom de service, à sélectionner du registre de services pour la forme de nom de service basé sur l'hôte GSSAPI.
2) Détail des négociations de mécanisme que le protocole fournis.
3) Définition des messages nécessaires pour l'échange d'authentification
4) Décrire la syntaxe de chaîne d'authorization identity non-vide
5) Détailler les facilité que le protocole fournis qui permettent au client/serveur d'annuler un échange
6) Identifier précisément où les couches de sécurité nouvellement négociée prenent effet.
7) Si le protocole supporte d'autres couche de sécurité tel que TLS, la spécification doit décrire l'ordre dans lequel les couches de sécurité sont appliquées dans les données du protocole
8) indiquer si le protocole supporte l'authentification multiple

Mechanism requirement

Les spécification des mécanisme doivent fournir les informations suivantes :

1) le nom du mécanisme
2) Si le mécanisme est client-first ou server-first.
3) si le serveur doit fournir des données additionnelles en indiquant une sortie réussie
4) Si le mécanisme est capable de transférer l'authorization identity
5) Si le mécanisme offre une couche de sécurité
6) si la technologie cryptographique utilisée supporte l'intégrité des données